Amendments to the Abstract

Please delete the Abstract appearing in the front page of the PCT publication and add the following new Abstract:

A method and device for performing a cryptographic operation by a device controlled by a security application executed outside thereof in which a cryptographic value (y) is produced a calculation comprising at least one multiplication between first and second factors containing a security key (s) associated with the device and a challenge number (c) provided by the security application. The first multiplication factor comprises a determined number of bits (L) in a binary representation and the second factor is constrained in such a way that it comprises, in a binary representation, several bits at 1 with a sequence of at least L-1 bits at 0 between each pair of consecutive bits to 1 while the multiplication is carried out by assembling the binary versions of the first factor shifted according to positions of the bits at 1 of the second factor, respectively.

A replacement Abstract is attached hereto on a separate sheet in accordance with 37 CFR 1.72.

ABSTRACT

A method and device for performing a cryptographic operation by a device controlled by a security application executed outside thereof in which a cryptographic value (y) is produced a calculation comprising at least one multiplication between first and second factors containing a security key (s) associated with the device and a challenge number (c) provided by the security application. The first multiplication factor comprises a determined number of bits (L) in a binary representation and the second factor is constrained in such a way that it comprises, in a binary representation, several bits at 1 with a sequence of at least L-1 bits at 0 between each pair of consecutive bits to 1 while the multiplication is carried out by assembling the binary versions of the first factor shifted according to positions of the bits at 1 of the second factor, respectively.